REMARKS

Claims 1, 2 and 4-6 are pending in the above-identified patent application. Claims 1 and 5 have been amended by way of the present amendment. Reconsideration is respectfully requested.

In the outstanding Office Action, claim 1 was objected to under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention; and claims 1, 2 and 4-6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,604,807 (Yamaguchi et al.) in view of "Transparent Network Security Policy Enforcement" (Keromytis et al).

35 U.S.C. § 112 Claim Rejections

Claim 1 was rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Reconsideration is respectfully requested.

Claim 1 has been amended to clarify the invention. In particular, claim 1 has been amended to replace "and/or" with the term "and." Therefore, it is respectfully submitted that the amendments raise no question of new matter and that claim 1, and claims dependent thereon are now definite.

35 U.S.C. § 103 Claim Rejections

Claims 1, 2 and 4-6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Yamaguchi et al. in view of Keromytis et al. Reconsideration is respectfully requested.

Claims 1 and 5 have been amended to clarify the invention. In particular, claim 1 and 5 have been amended to recite:

> a manager terminal for inputting ~~various information for controlling encrypted-data communications~~ information for the

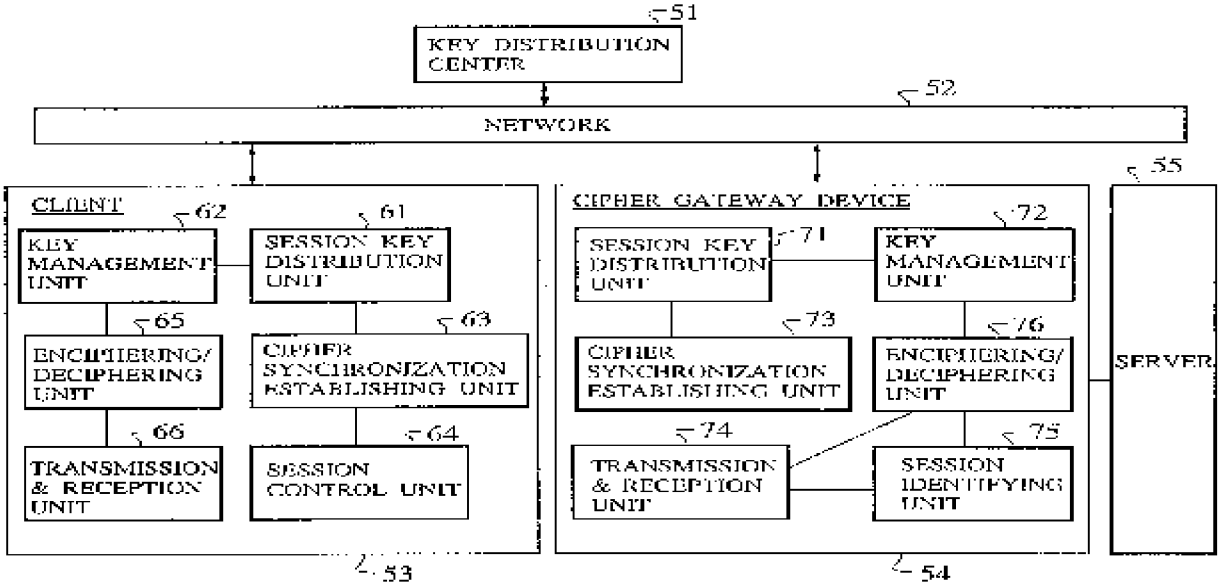
> presence or absence of encryption/decryption process, the availability of packet communications, the encryption level, the time period to perform encryption, the encryption policy, and the encryption key into each of the encryption apparatus and the communications terminals remotely from the manager terminal over a network, so that settings for the encrypted data communications on each of the apparatus and the terminals are completed

Support for the amendment is provided in the original application and figures. In particular, the specification discloses: "a manager terminal **12** to each of the encryption apparatus **1** and the PCs **7-9** via the hub **5**, wherein examples of the information to be set by the manager terminal includes: (A) Information that instructs to perform the encrypting/decrypting process, or instructs not to perform the encrypting/decrypting process; (B) Information for instructing to discard data packets (In particular, this information instructs to discard data packets, when data packets to be communicated between predetermined terminals have been received.); (C) Information for instructing a security level of the encryption; (D) Information for instructing time when data encryption is to be performed; (E) The encryption policy for each division; and (F) Information for encryption keys.[1]

Yamaguchi et al. discloses a cipher communication system and scheme capable of realizing the cipher communication without affecting the already existing application programs and hardware, and establishing a synchronization at the start and end of the cipher communication.[2] In particular, Yamaguchi et al. discloses, as shown in **FIG. 12** below, wherein each client **53** and each cipher gateway device **54** are connected with the key distribution center **51**, the network **52**, and the server **55**.[3] Further, Yamaguchi et al. discloses the cipher gateway

[1] U.S. Patent Application Publication No. 20050008160 at paragraphs **[0035]** to **[0041].**
[2] Yamaguchi et al. at ABSTRACT.
[3] *Id.* at **FIG. 12**; and column 10, lines 53-56.

FIG. 12



device **54** or router receives the packet destined to the server **55** from the client **53**, and deciphers the packet by using the common session key Ks and that this deciphered packet (plain text packet) is transmitted to the server **55** to carry out the non-cipher communication between the cipher gateway device **54** and the server **55**.[4] Alternatively, Yamaguchi et al. discloses the cipher gateway device **54** or router receives the packet destined to the client **53** from the server **55** by the non-cipher communication, and enciphers the packet by using the common session key Ks and this enciphered packet is transmitted to the client **53** to carry out the cipher communication between the cipher gateway device **54** or router and the client **53**.[5]

However, Yamaguchi et al. nowhere discloses, as amended claims 1 and 5 recite:

> *a manager terminal for inputting information for the presence or absence of encryption/decryption process, the availability of packet communications, the encryption level, the time period to perform encryption, the encryption policy, and the encryption key* into each of the encryption apparatus and the communications terminals remotely from the manager terminal

[4] *Id.* at **FIG. 12**; and column 12, lines 50-56.
[5] *Id.* at **FIG. 12**; and column 12, lines 57-63.

> over a network, so that settings for the encrypted data communications on each of the apparatus and the terminals are completed (emphasis added).

That is, Yamaguchi et al. nowhere discloses a management system in the network security communication and centrally managed by a manager terminal as claimed or the necessary and sufficient information (i.e., all security policies such as for whether to perform encryption, availability of communication itself, for example, to abandon packets between specific terminals, encryption level, time period to perform encryption, encryption policy, and encryption key) to perform each secure communication between terminals. Thus, it is respectfully submitted that Yamaguchi et al. does not disclose these limitations of the claimed invention.

In addition, the outstanding Office Action acknowledges other deficiencies in Yamaguchi et al. and attempts to overcome these deficiencies by combining Keromytis et al. with Yamaguchi et al. However, Keromytis et al. cannot overcome all of the deficiencies of Yamaguchi et al. as will be discussed below.

Keromytis et al. discloses recent work in the area of the network security, such as IPsec, provides mechanisms for securing the traffic between any two interconnected hosts.[6] However, Keromytis et al. does not disclose the mechanism of the central encryption management, but just the combinations between encryption communications and bridges. In particular, Keromytis et al. does not disclose, as amended claims 1 and 5 recite:

> *a manager terminal for inputting information for the presence or absence of encryption/decryption process, the availability of packet communications, the encryption level, the time period to perform encryption, the encryption policy, and the encryption key* into each of the encryption apparatus and the communications terminals remotely from the manager terminal over a network, so that settings for the encrypted data communications on each of the apparatus and the terminals are completed (emphasis added).

[6] Keromytis et al. at ABSTRACT.

That is, configurations to centrally manage by a "manager terminal" necessary and sufficient information in order to perform each secure communication between terminals in the network are not disclosed by either in Yamaguchi et al. and Keromytis et al. Thus, the configurations of the central encryption management system in the claimed invention that enable necessary and sufficient information to be distributed and that is also transparent to the IPsec bridge to perform secure communication, is not disclosed, suggested or make obvious by either Yamaguchi et al. nor Keromytis et al., whether taken alone or in combination. Therefore, it is respectfully submitted that claims 1 and 5 patentably distinguish thereover.

Conclusion

In view of the above, consideration and allowance are respectfully solicited.

In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 22040-00038-US1 from which the undersigned is authorized to draw.

Dated: May 20, 2008

Respectfully submitted,

Electronic signature: /Myron Keith Wyche/
Myron Keith Wyche
Registration No.: 47,341
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 293-6229 (Fax)
Agent for Applicant